

**U.S. DEPARTMENT OF STATE
BUREAU OF CYBERSPACE AND DIGITAL POLICY (CDP)**

**Notice of Funding Opportunity (NOFO):
Foreign Assistance Leveraged for Cybersecurity Operational Needs (FALCON)**

This is the announcement of funding opportunity number DFOP0016632.

Federal Assistance Listing/Catalog of Federal Domestic Assistance Number: 19.665

Type of Solicitation:	Open Competition
Deadline for Applications:	11:59 PM EDT on Friday 9 August 2024
Total Funding:	\$10,000,000
Funding Type:	Economic Support Funds (ESF) Creating Helpful Incentives to Produce Semiconductors(CHIPS) Act of 2022/ International Technology Security and Innovation (ITSI) Fund
FADR Data Element 1:	EG.8 Global
Anticipated Number of Awards:	1 to 3 awards are anticipated
Type of Award:	Cooperative Agreement
Period of Performance:	36 months
Anticipated Time to Award:	August 2024
Deadline for Questions:	11:59 PM EST on Monday 22 July 2024
Eligibility Category:	U.S.- based non-profit/non-governmental organizations subject to sections 501 (c)(3) and 501 (c)(6) of the U.S. tax code or U.S. for- profit organizations or businesses.

Type of Applicant:	Organizations only. Individuals not eligible to apply.
Number of Applications:	One (1) per applicant organization.

This notice is subject to availability of funding.

Section A: Project Description

The U.S. Department of State, Bureau of Cyberspace and Digital Policy (CDP) is pleased to announce an open competition for organizations with the capacity and interest to carry out the program outlined in this announcement.

Pending the availability of funds, CDP anticipates awarding one (1) to three (3) cooperative agreements of up to \$10,000,000.00 USD in total. CDP reserves the right to award more or less funding or make no award as is in the best interest of the US Government.

A1. Background of CDP/DCCP

CDP promotes U.S. national and economic security by leading, coordinating, and elevating foreign policy on cyberspace and digital technologies. It builds partnerships to shape the international environment so Americans and people everywhere can prosper. CDP strives for a world in which every person can access the opportunities that come with digital connectivity to build thriving economies and societies and works to counter challenges to this vision from authoritarian states.

Recognizing the growing role of technology as a cross-cutting national security issue, the State Department created CDP in April 2022 to lead and coordinate U.S. diplomacy on cyber and digital policy. CDP addresses the national security challenges and economic opportunities presented by cyberspace and digital technologies and promotes standards and norms that are fair, transparent, and support the rights-respecting use of technology. Through robust engagement in multilateral organizations, bilateral diplomacy with partners around the world, and encouragement of responsible state behavior in cyberspace, CDP empowers U.S. leadership in cyber, digital, and technology diplomacy.

CDP deploys foreign assistance funding to strengthen international cooperation, create new partnerships, promote economic growth and development, and assist in the defense of our foreign partners to uphold an open, interoperable, secure, and reliable Internet.

Calibrated cyber and digital policies help form the backbone of our deeply interconnected world, are vital to U.S. national and economic security, and are required to fully harness the transformative power of technology. As citizens around the world eagerly seek increased Internet connectivity to access the tremendous opportunities afforded by digital transformation, the United States is working to ensure this connectivity is secure, meaningful, governed fairly, and serves the interests of its users. Foreign assistance programs aim to advance an affirmative vision of technology as a tool that supports collective security, prosperity, and democratic values.

More information on CDP is available at <https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/>.

The Digital Connectivity and Cybersecurity Partnership (DCCP) is a global, interagency initiative led by CDP and the U.S. Department of State to promote an open, interoperable, secure, and reliable internet. DCCP provides foreign assistance to partner nations to promote investments in secure, diverse, and resilient information and communication technologies (ICT) infrastructure; support the adoption of inclusive, rights-respecting, multi-stakeholder models of internet governance; grow global markets for trusted ICT goods and services; and enhance cybersecurity. CDP foreign assistance programming follows these core tenets of DCCP. More information on DCCP is available at <https://www.state.gov/digital-connectivity-and-cybersecurity-partnership/>.

A2. Applicable CDP Strategic Program Goals and Objectives

CDP Strategic Goals and Objectives:

Bureau Goal 1: Advance cyber and digital policies that align with U.S. national interests and foreign policy objectives.

- **Objective 1.1:** Deepen relationships with existing U.S. allies and partners, forge new partnerships, and engage with a range of countries to advance a common vision for the Internet and digital technologies.
- **Objective 1.3:** Identify, enhance, cultivate, and develop strategic engagements across the private sector and multistakeholder communities.
- **Objective 1.4:** Increase secure and open digital connectivity and access to the Internet.

DCCP Pillars:

Pillar 1: Build Connections by promoting investments in secure, diverse, and resilient ICT infrastructure.

Pillar 2: Advance an Open, Interoperable, Reliable, and Secure Internet by promoting inclusive, rights-respecting, multi-stakeholder models of internet governance and pro-competition, pro-innovation digital economy policies and regulations.

Pillar 3: Grow Global Markets for U.S. ICT goods and services, especially high-quality, interoperable, secure ICT equipment, software, and services.

Pillar 4: Enhance Cybersecurity by increasing adoption and implementation of cybersecurity best practices.

CHIPS Alignment

Through DCCP, the State Department leads the U.S. government's efforts to advance the adoption of secure and trustworthy ICT infrastructure and to defend against malicious cyber activity abroad. Using resources from the CHIPS/International Technology Security and Innovation (ITSI) Fund, appropriated under the CHIPS Act of 2022, CDP will engage with select partners to provide cybersecurity tools and services to better manage cybersecurity threats to allied and partner networks and infrastructure.

The FALCON project also aligns with objective 5.3.2 of the National Cybersecurity Strategy Implementation Plan: "Establish flexible foreign assistance mechanisms to provide cyber incident response support quickly."

A3. Project Goals, Objectives, Expected Outcomes, Activities, Indicators, and Sustainability

CDP's Foreign Assistance Leveraged for Cybersecurity Operational Needs (FALCON) project is intended to establish and maintain a reservoir of primarily commercial cybersecurity and technology capabilities that CDP can draw upon in short order and in a wide variety of situations to support U.S. allies and partners to effectively prevent, respond to, mitigate, and recover from cybersecurity incidents.

The objective of the project is to support partner governments, their subordinate agencies and critical infrastructure operators and partners in their efforts to identify, prevent, respond to, mitigate and recover from cybersecurity incidents. Assistance implemented under FALCON will be in alignment with Section A2 above.

Project Objectives

CDP seeks applications from organizations that are well poised to:

Objective 1 - Deploy crisis and non-crisis incident prevention and response resources, as well as other appropriate assistance, on relatively short notice.

Objective 2 – Design and implement short-to-medium-term technical assistance – including but not limited to strategic or technical advisement, procurement, or remediation support.

FALCON award recipients may be required to work virtually, in person, or both. They should be prepared to work in close coordination with CDP, the Department and the U.S. interagency, and to deploy technical assistance and/or procure and deploy equipment including software and hardware as tailored to each engagement. Recipients should propose consortiums or partnerships to be able to rapidly subcontract or subaward for a broad array of subject matter experts, companies or other providers for cyber technical good and services.

CDP Intended Project Outcomes

Outcome 1 - Governments or beneficiaries can effectively prevent, respond to, and mitigate cyber incidents while respecting human rights.

Outcome 2 - Partner country or beneficiaries can safely use the Internet and their privacy is safe-guarded.

Project Design

Project activities will be initiated by CDP on a rolling basis via summary **Project Activity Scopes (PAS – see Tab 4)**. Each PAS will include as much information as is available at the time of submission and will request the recipient to either scope and cost the activity or to cost the activity to the scope provided by CDP. Recipient should be prepared to coordinate with State, affected foreign entities, and other stakeholders and partners to conduct an initial virtual scoping effort. This may include soliciting information, deploying virtual diagnostic software or remotely coordinating its on-the-ground deployment, and/or undertaking remote digital forensics efforts. The outcome should include a working assessment of the incident and its severity, and a set of initial recommendations for next steps and remediation and a time and cost estimate as appropriate. If appropriate and directed by CDP, the recipient should be prepared to effectively hand-off the incident to another team or set of partners for further investigation and/or remediation.

Project activities may include but are not limited to the following:

- Cyber Incident Scoping
- Cyber Incident Response
- Cyber Incident Mitigation
- Cybersecurity Technical Assistance

- Rapid Procurement and Deployment of Products and Technologies
- Short-term Advisory Services and Research
- Short-term Training

The successful applicant(s) will clearly demonstrate their ability to provide or acquire (in a timely manner) the correct subject matter experts, technical equipment, and/or services required for each type of potential project activity illustrated above or will specify which are outside of their remit. The applicant should also demonstrate their experience with federal contracting and logistics management.

A successful application to this announcement will describe the organization's experience or abilities to respond to each of the following types of scenarios. This list is not inclusive and is provided for illustrative purposes:

- Respond, in some cases within 6 (six) hours, to initial CDP outreach identifying a potential emergency or urgent cyber incident to begin initial discussions of the incident at hand. Following that outreach, recipient should then be prepared to begin coordinating with State, affected foreign entities, and other stakeholders and partners to conduct an initial and/or ongoing scoping effort to the contours defined in the first paragraph of the Project Design section above.
- Advise and assist partner government agencies, their subordinate agencies and critical infrastructure operators' capability to harden and defend critical assets and systems, while evolving their capability to sustain these solutions post-intervention. This may include virtual or in-person assessments, the rapid procurement and deployment of technical solutions including for detection and monitoring of suspicious behavior, virtual advisory or training calls, or issuance of recommendations and support for their implementation.
- Directly conduct a wide variety of virtual and in-person incident and crisis response support, including but not limited to commanding/managing relevant elements of the overall response. This may involve working side-by-side with local owners and operators, local employees, and other entities as appropriate. It may require coordination with elements of business, legal, government, media, finance, or other personnel as appropriate, and coordinate efforts to support the continuity of critical operations by restoring services, providing back-ups or coordinating with other entities may further require recipients to assess the risk and impact to critical systems and triage accordingly.
- Conduct network assessments, scan for vulnerabilities, find or analyze malicious software (malware), and/or identify other problems – and enumerate, procure, and deploy the appropriate and trusted tools, services or solutions to remediate. This may require acquiring alternative methods of connectivity, including

portable high-speed mobile broadband, to work in areas in which networks are compromised or otherwise not reliable.

- Share threat information with the broader community as appropriate. Improve information sharing of threats and incidents, through established networks and formal/informal procedures, between national and industry counterparts throughout the region and with the United States. Information-sharing may follow because of an engagement or separately.
- Support and develop the ability of host government agencies and critical infrastructure owners and operators to procure, integrate and maintain hardware and software solutions; to scope, develop, and implement technical processes and strategies; to restructure, as appropriate, existing systems, network architecture, configurations, or security practices. This may be undertaken with or without a triggering cybersecurity incident.
- Cooperate with the U.S. government and with host government agencies and critical infrastructure owners and operators to, as appropriate, establish the grounds for an engagement within the country – which may include guidelines for how information will be shared and maintained, the creation of NDAs or MOUs to scope and shape the terms of the encounter, and to clearly delineate the cessation or extension, as appropriate, of support following the conclusion of an activity.

The recipient will deliver the appropriate cybersecurity assistance to the beneficiary, impacted government or critical infrastructure operating team, as agreed upon in the PAS. This may be conducted virtually, in-person, or through a hybrid combination. If in-person support is necessary, the implementers must be capable of deploying within the timeline established by the U.S. Department of State, which may require departing as rapidly as 48 (forty-eight) hours from approval of the PAS.

Applicants must demonstrate existing – or the capacity to develop – working relationships with local in-country partners, entities, and relevant stakeholders, and have demonstrable experience in administering successful and preferably similar technical projects. Applicants must also demonstrate the ability to draw on a range of trained cybersecurity and other professionals prepared to adhere to the highest personal and professional standards; to acquire or maintain, as appropriate, security clearances and access to classified systems; and to work outside of normal working hours and in possible austere or difficult conditions that may require the use of atypical tools, translation services, or other logistical challenges. Recipients will be required to coordinate with CDP on each PAS to ensure the use of trusted solutions and vendors (i.e. the composition of the “tech stack”).

Project Process

A draft PAS is provided and attached to this NOFO (See **Tab 4 – FALCON Project Activity Scope**). The summary PAS will provide a description of CDP's request and/or approach for each FALCON project activity. Upon receipt of the PAS, the recipient will be required to complete a narrative that describes the needs, scope, scale, and response or solution proposed; a discrete budget; a logic model and monitoring and evaluation plan; and a risk, and sustainability assessments. For the sake of expediency, collaboration with CDP during this phase is expected and encouraged. The recipient will complete and return the PAS to CDP program officials for review and approval within 7 business days in non-crisis situations. In crisis situations in which a rapid deployment is requested (as defined by CDP program officials) or when little technical data about the request is known, the PAS may be submitted on a preliminary basis and simplified temporarily to include only the proposed immediate response and budget estimate. In this case, a more fulsome PAS will be required at a date no later than established by the CDP program officials. No work shall commence on a PAS until the recipient and CDP agree and sign off on the completed PAS. A PAS may be amended as needed and as agreed to in writing by CDP and the recipient.

In every case the completed PAS will contain, at a minimum, the following sections.

FALCON PAS Narrative: Recipient will prepare a project narrative that expands or explains the proposed project solution or intervention as appropriate and will detail and justify the proposed activities to take to achieve the desired outcome. The narrative shall have a separate discussion of risk analysis and risk mitigation strategy and should include an expectation of the types of telemetry or other associated data they anticipate receiving and how it will be handled. The narrative shall also have a separate discussion concerning what the sustainability of the interventions would look like, how it could be resourced and any other relevant factors that necessarily need to be considered (see **Tab 4 – FALCON Project Activity Scope**).

FALCON PAS Logic Model: Recipient will be required to complete a PAS Logic Model for each approved Project Activity Scope (see **Tab 5 – FALCON PAS Logic Model**).

FALCON PAS Budget: Using the budget template with definitions provided (See **Tab 6 FALCON Detailed Budget for PAS**), the recipient will cost only the project described in the PAS in accordance with the activities, including monitoring and evaluation, proposed. The budget should include all associated sub-award and indirect and overtime costs. A PAS Budget Narrative will also be required. See Budget Development and Reporting above.

FALCON PAS Performance Monitoring and Evaluation Plan: will be required to complete the document **at Tab 7 – FALCON PAS Performance Monitoring and Evaluation Plan**. The document will detail how the project activity performance will be monitored and evaluated and who will carry out this function. It will:

- Explain how the project activity's performance toward its objectives will be tracked over time.
- Identify which performance indicators the project activity will report against, the indicator type, baseline values, performance targets, and data sources and collection methods.
- Provide a clear description of the approach and data collection strategies and tools to be employed (e.g., pre- and post-test surveys, interviews, focus groups).
- Identify what, if any, external evaluations will be conducted.
- Risk Analysis: Internal and external risks associated with the proposed project, rate the likelihood of the risks, rate the potential impact of the risks on the project, and identify actions that could help mitigate the risks. -
- Sustainability: Please specify how the project will empower the beneficiary country to sustain solutions and to bolster cybersecurity capacity in the mid-to-long term - including how the implementer anticipates tapering direct foreign assistance.

A4. Key Considerations

Strong preference will be given to applicant(s) (see section E.1 Evaluation Criteria for additional information) that:

- Demonstrate highly developed administrative, logistical, and technical capacity and experience in administering successful and similar projects with a global participant base.
- Outline their expedited procurement procedures, capacity to deploy remote or virtual cyber incident diagnostics, ability to assess and implement remediation measures (including clearing networks), and other key indicators of technical ability.
- Demonstrate thoughtful project design capacity to address the key objectives and activities for the target beneficiaries – as well as flexibility in deploying effective and durable solutions according to understood best practices.
- Demonstrate capacity to develop and execute logic models and monitoring and evaluation and report results.
- Prove existing, collaborative, and successful partnerships with U.S. and foreign partners on issues and engagements related to cybersecurity and digital policy.

- Demonstrate capacity to deploy complex technical solutions in response to sophisticated cyber threat activity.
- Demonstrate adherence to ethical best practices including “do no harm” and gender equity with respect to project activities.

All applicants will also be required to address **the entirety of Sections A.3 and A.4** within this NOFO in their application.

Section B: Federal Award Information

Organizations may submit one application per organization in response to this NOFO. If more than one application is submitted by an organization, only the first application received will be reviewed for eligibility and funding.

The U.S. government reserves the right to: (a) reject any or all applications, (b) accept other than the lowest cost application, (c) accept more than one application, and (d) waive irregularities in applications received.

The U.S. government may make award(s) based on initial applications received, without discussions or negotiations. Therefore, each initial application should contain the applicant's best terms from a cost and technical standpoint. The U.S. government reserves the right (though it is under no obligation to do so), to enter discussions with one or more applicants in order to obtain clarifications, additional detail, or to suggest refinements in the project description, budget, or other aspects of an application.

CDP anticipates awarding one or more Cooperative Agreements. The final determination on award mechanism will be made by the Grants Officer.

The authority for this funding opportunity is found in the Foreign Assistance Act of 1961 (FAA), as amended. Several funding restrictions apply, to include country restrictions. Initial program funding is provided via the Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act of 2022.

To maximize the impact and sustainability of the award(s) that result(s) from this NOFO, CDP reserves the right to execute a non-competitive continuation amendment(s). The total duration of any award, including potential non-competitive continuation amendments, shall not exceed 54 months, or four and a half years. Any non-competitive continuation is contingent on availability of funds, and satisfactory performance of the

program. A non-competitive continuation is not guaranteed, and the Department of State reserves the right to exercise or not exercise this option.

The distinction between grants and cooperative agreements revolves around the existence of “substantial involvement.” Cooperative agreements require greater federal government participation in the project. If a cooperative agreement is awarded, CDP will undertake reasonable and programmatically necessary substantial involvement. Examples of substantial involvement could include but are not limited to:

- Active participation or collaboration with the recipient in the implementation of the award.
- Review and approval of one stage of work before another can begin.
- Collaboration on selection and/or review and approval of sub-award partnerships or sub-contracts beyond existing federal policy.
- Approval of the recipient’s budget or plan of work prior to the award.
- Review participant training program acceptance and rejection letters.

Section C: Eligibility Information

C1. Eligible Applicants

CDP welcomes applications from U.S.-based non-profit organizations subject to section 501(c)(3) and 501(c)(6) status of the U.S. tax code and U.S. for-profit organizations.

Applications submitted by for-profit entities may be subject to additional review following the Merit Review Panel selection process. Additionally, applicants may not earn or keep any profit resulting from Federal financial assistance, unless explicitly authorized by the terms and conditions of the Federal award. Profit is defined as any amount in excess of allowable direct and indirect costs. The allowability of costs incurred by commercial organizations is determined in accordance with the provisions of the Federal Acquisition Regulation (FAR) at 48 CFR 30, Cost Accounting Standards Administration, and 48 CFR 31 Contract Cost Principles and Procedures.

C2. Cost Sharing or Matching

Providing cost sharing, matching, or cost participation **is not** an eligibility factor or requirement for this NOFO and providing cost share will not result in a more favorable competitive ranking.

Per 2 CFR §200.306, items that are proposed for cost share must be allowable per 2 CFR §200, Subpart E—Costs Principles.

C3. Other

To be eligible to receive an award, all organizations must have a unique entity identifier (UEI), as well as a valid registration on [SAM.gov](https://sam.gov). Please see Section D3.2 for information on how to obtain these registrations.

Applicants must be organizations, and only one application will be considered for each applicant organization. If more than one application is submitted by the same organization, only the first received will be reviewed for eligibility and funding.

Please note, any applicant listed on the Excluded Parties List System in the [System for Award Management \(SAM.gov\)](https://sam.gov) and/or has a current debt to the U.S. government is not eligible to apply for an assistance award in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR, 1986 Comp., p. 189) and 12689 (3 CFR, 1989 Comp., p. 235), “Debarment and Suspension.” Additionally, no entity or person listed on the Excluded Parties List System in SAM.gov can participate in any activities under an award. All applicants are strongly encouraged to review the Excluded Parties List System in SAM.gov to ensure that no ineligible entity or person is included in their application.

Section D: Application and Submission Information

D1. Address to Request Application Package

Application forms, and other required materials are available at Grants.gov (<http://www.grants.gov>) and MyGrants (<https://mygrants.servicenowservices.com>) under the announcement title “FALCON”, and funding opportunity number “DFOP0016632”. Once the NOFO deadline has passed, the Department of State may not discuss this competition with any applicant until the proposal review process has been completed. If requesting reasonable accommodations for persons with disabilities or for security reasons, please contact the CDP point of contact listed in Section G. Please note that reasonable accommodations do not include deadline extensions.

D2. Content and Form of Application Submission

For all application documents, please ensure:

- The proposal clearly addresses the goals and objectives of this funding opportunity, and describes the organization's capabilities as described in sections A.3 and A.4.
- All documents are in English
- All budgets are in U.S. dollars
- For documents subject to page limitations, all pages are numbered
- All documents are formatted to 8 ½ x 11 paper and,
- All Microsoft Word documents are single-spaced, 12-point Calibri font, with a minimum of 1-inch margins
- Captions and footnotes may be 10-point Calibri font

Any prospective applicant who has questions concerning the contents of this NOFO should submit them by email to the contacts listed in Section G. Any updates about this NOFO will be posted on [Grants.gov](https://www.grants.gov).

D2.1 Application Requirements

Complete applications must include the following:

1. Completed and signed **SF-424**, **SF-424A**, as well as **SF-424B**, if applicable.
2. Organizations that engage in lobbying the U.S. government, including Congress, or pay for another entity to lobby on their behalf, are also required to complete the **SF-LLL "Disclosure of Lobbying Activities"** form.
3. **Cover Page** (one page). Includes the organization name, application title, and name and contact information for the application's main point of contact.
4. **Proposal Narrative** (not to exceed seven [7] pages, preferably as a Word Document). The Proposal Narrative must include the following:
 - **Introduction to the Organization:** Description of past and present operations, showing applicant's ability to carry out the project, including information on relevant or similar type projects from previous grants from CDP and/or U.S. government agencies.
 - **Statement of Capabilities and Experience:** Clear, concise, and well-supported statement that fully describes the applicant's unique project/approach will address both FALCON objectives and support CDP's Strategic Goals and Objectives. Applicant should describe past experience with Federal contracting and logistics management, industry knowledge and contacts.

- **Risk Analysis:** Internal and external risks associated with the project, including an assessment of any anticipated risks, the likelihood of those risks, and actions that could help mitigate the risks. Please also provide an overview of the applicant's ability to monitor and evaluate the project and address sustainability solutions.

Please note the seven-page limit does not include the following:

- SF-forms listed above
- Cover Page
- FALCON Detailed Budget – Baseline (**see below, and Tab 1**)
- FALCON Budget Narrative – Baseline (**see below, and Tab 2**)
- FALCON Strategic Scope of Work (**see below, and Tab 3**)
- Key Personnel Information, CVs or Resumes (per person)
- Additional Required Attachments (Audit, NICRA, etc.)

5. FALCON Detailed Budget Baseline (Excel workbook strongly preferred; please **do not** provide as a PDF).

The applicant(s) should prepare a 'baseline' or retainer budget that includes a subject matter expert program manager, an agreements or contracts specialist, and a budget officer for the duration of the period of performance. (See **Tab 1 FALCON Detailed Budget – Baseline**). This baseline budget should also include all overhead costs and fringe benefits associated with these costs. CDP envisions that this budget will be constant at a pre-determined level throughout the performance period of the award and will be augmented by proposed PAS budgets. Applicants should provide a detailed description of the applicant's personnel overtime policy and any other personnel policies that could impact the budget given the rapid response nature of program activities in the Budget Narrative. Applicants should also include this information for partner organizations.

Please note that, separately, costing and staffing individual PAS activities will be required on a rapid response basis. Recipient(s) will be required to reconcile to each approved PAS budget as a project activity and include the reconciliation in the required performance reports. Recipient will be required to report against the budget categories contained in the Standard Form 424A application from both the PAS budget(s) and the baseline budget categories combined.

Include three (3) columns containing the baseline request to CDP (see Program Design above), any cost sharing contribution, and the total budget. A Summary Budget should also be included using the OMB-approved budget categories (see SF-424A as a sample) in a separate tab. Costs must be in U.S. Dollars.

6. **FALCON Budget Narrative – Baseline** (preferably as a Word Document).

A Budget Narrative is also required that explains any “downtime draw” during periods in which CDP is not drawing on the recipient’s services through individual projects. Justify each line-item in the **baseline** budget and explain how the amounts were derived, consistency with the applicants’ documented policies, as well as the source and description of all proposed costs (and cost-share, if applicable). The narrative should complement the budget rather than repeat information provided in the budget. For example, the narrative should provide details on the purpose of costs, reasonability of costs, cost price analysis; explain allocations and any yearly variances; and tie expenses to project activities and/or objectives where appropriate. Sources of all cost-share offered in the application should be identified and explained in the budget narrative.

See Tab 1 FALCON Detailed Budget – Baseline for budget instructions and Tab 2 FALCON Budget Narrative – Baseline Instructions.

7. **FALCON Strategic Scope of Work**

Please describe at a high level your organization’s proposed approach to operationalize your capabilities to meet FALCON objectives and achieve CDP top-level goals. This may include an assessment of your organization's particular strengths and niche relationships, or accomplishments. In short, when confronted with a hypothetical Project Activity Scope how does your organization propose to respond and what would your process entail. We seek insight into your organizational perspective. (See **Tab 3 FALCON Strategic Scope of Work**).

8. List of Key Personnel and Subject Matter Experts (overall, not to exceed ten [10] pages, preferably as a Word Document). CDP envisions the successful applicants will propose an experienced subject matter expert as the program manager, a highly qualified financial officer, and highly qualified contracting officer with substantial experience sub-awarding USG funds. The above key personnel will comprise the core staff of the project. A one-page resume for each of these individuals is required in the application, in addition to a short description of their areas of subject matter expertise and what qualifications or metrics were used in this determination. CDP envisions the successful applicant will have extensive contacts and relationships within the ICT and cybersecurity industry and will be able to reach out and execute appropriate agreements with these entities in an expeditious manner in order to execute approved Project Activity Scopes. This list can represent staff within the applicant’s organization or outside of the organization (subgrantee, consultants, contractors), who are potentially integral to the success of a given project. The list should provide names, titles, roles, and one paragraph bios that highlight relevant experience/qualifications of personnel and

subject matter experts who may be called upon to become involved in a project activity. It should also specify their working relationship to the recipient and previous work together – noting that applicants able to demonstrate existing relationships with a broad grouping of vendors able to meet the requirements will be evaluated more favorably. As appropriate, the personnel and subject matter experts should specify skillsets and capabilities, including but not limited to: (1) incident response and remediation, (2) incident management (including non-technical skills), (3) cyber threat expertise and assessment, including forensics, (4) defensive cyber operations, (5) network security, (6) penetration testing, (7) hardware and software deployment.

9. Additional Required Attachments:

- **Audit:** An audit or an explanation for the lack of an audit is required. Please review the bulleted items below carefully.
 - If your organization meets the threshold as defined in 2 CFR 200 Subpart F, then your organization must submit a PDF of its most recent 'single audit'.
 - If your organization does not currently meet the 2 CFR 200 requirement and has not had a 'single audit' within the last three fiscal years, then your organization must submit its most recent audit (within the last three years) independent financial audit, as a PDF.
 - If your organization has not been independently audited within the last three years, then it must explain the reason for the lack of an audit and provide an independent confirmation of the adequacy of its internal controls.
- **Negotiated Indirect Cost Rate Agreement (NICRA):** Your latest NICRA letter should be included as a PDF file if your organization has a NICRA and includes NICRA charges in the budget. This document will not be reviewed by the Merit Review Panel but will be used by project and grant team if the submission is recommended for funding. Organizations that have previously established indirect cost rates must submit timely indirect cost proposals to their cognizant agency as required by Appendix III & IV of 2 CFR 200. If indirect cost proposals have not been submitted for re-negotiation, as required, out-of-date NICRAs may not be considered. If your proposal involves subawards to organizations charging indirect costs, please submit their NICRA, if applicable.
- **Letters of support** from any partner or partners identified in the proposal whose role is central to the project achieving its objectives should describe the roles and responsibilities of each partner. No letter of support is required for goods or services that are widely available commercially.

Applications that do not include the elements listed above will be deemed technically ineligible. To ensure that all applications receive a balanced evaluation, the review panel will review from the first page of each section up to the page limit and no further.

D.2.2 Additional Information Requested for Those Receiving Conditional Notification Letter

Successful applicants must submit, after Conditional Notification Letter, but prior to issuance of a federal award:

- Written responses and revised application documents addressing conditions and recommendations from the review panel.
- If not previously provided, a copy of the applicant's latest NICRA as a PDF file, if the applicant has a NICRA and includes NICRA charges in the budget.
- A completed copy of the Department's Financial Management Survey, if receiving USG funding for the first time.
- Submission of required documents to register in the Payment Management System managed by the Department of Health and Human Services, if receiving CDP funding for the first time.
- Other requested information or documents included in the Conditional Notification Letter or subsequent communications prior to issuance of a federal award.
- Applicants who submit their applications through Grants.gov will be required to create a MyGrants account in order to accept the final award. Accounts must be logged into to every 60 days in order to maintain an active account.

D3. Unique Entity Identifier (UEI) and System for Award Management (SAM)

All organizations must have a Unique Entity Identifier (UEI) and an active registration with SAM.gov. A UEI is one of the data elements mandated by Public Law 109-282, the Federal Funding Accountability and Transparency Act (FFATA), for all federal awards.

The 2 CFR 200 requires that sub-grantees obtain a UEI number. Please note the UEI for sub-grantees is not required at the time of application but will be required before an award is processed and/or directed to a sub-grantee.

Note: The process of obtaining or renewing a SAM.gov registration may take anywhere from 4-8 weeks. Please begin your registration as early as possible and advise proposed sub-grantees to do so as well.

Organizations **based in the United States** will need an Employer Identification Number (EIN) from the Internal Revenue Service (IRS) and a UEI number issued through SAM.gov. Once the UEI number is received continue with the remainder of the SAM.gov registration.

Note: SAM.gov is not the same as MyGrants. It is free to register in both systems, but the registration processes are different.

Please note, guidance on SAM.gov and the guidance on GSA's website about requirement for registering in SAM.gov is subject to change at any time. Applicants should review the website frequently for the most up-to-date guidance.

D3.1 SAM.gov and UEI Exemptions

An exemption from the UEI and sam.gov registration requirements may be permitted on a case-by-case basis if:

- An applicant's identity must be protected due to potential endangerment of their mission, their organization's status, their employees, or individuals being served by the applicant.
- For an applicant, if the federal awarding agency makes a determination that there are exigent circumstances that prohibit the applicant from receiving a unique entity identifier and completing SAM.gov registration prior to receiving a federal award. In these instances, federal awarding agencies must require the recipient to obtain a unique entity identifier and complete SAM.gov registration within 30 days of the federal award date.

Organizations requesting exemption from UEI or SAM.gov requirements must email the point of contact listed in Section G of the NOFO at least **two weeks prior to the deadline in the NOFO providing a justification of their request**. Approval for a SAM.gov exemption must come from the warranted Grants Officer before the application can be deemed eligible for review.

D3.2 Registering in MyGrants and Grants.gov

All application submissions must be made electronically via [Grants.gov](https://grants.gov) or MyGrants (<https://mygrants.servicenowservices.com/ilms/>). Both systems require registration by the applying organization. Please note that the Grants.gov registration process can take ten (10) business days or longer, even if all registration steps are completed in a timely

manner. Instructions for registering and submitting applications in each system are provided below.

MyGrants:

Applicants using MyGrants for the first time should complete their “New Organization Registration.” To register with MyGrants, go to:

<https://mygrants.servicenowservices.com> and click “create an account”.

Please note that establishing an account in MyGrants may require the use of smartphone for multi-factor authentication (MFA). If an applicant does not have accessibility to a smartphone during the time of creating an account, please contact the helpdesk and request instructions on MFA for Windows PC.

Organizations **must** remember to save a screen shot of the checklist showing all documents submitted in case any document fails to upload successfully.

MyGrants Help Desk:

For assistance with MyGrants accounts and technical issues related to the system, please contact the ILMS help desk by phone at +1 (888) 313-4567 (toll charges apply for international callers) or through the Self-Service online portal that can be accessed from <https://mygrants.servicenowservices.com>. Customer support is available 24/7.

Grants.gov:

Applicants who do not submit applications via MyGrants may submit via [Grants.gov](https://www.grants.gov). Please be advised that completing all the necessary registration steps for obtaining a username and password from Grants.gov **can take ten (10) business days or longer**.

Please refer to the Grants.gov website for definitions of various “application statuses” and the difference between a submission receipt and a submission validation. Applicants will receive a validation e-mail from Grants.gov upon the successful submission of an application. Validation of an electronic submission via Grants.gov can take up to two business days. Additionally, organizations **must** remember to save a screenshot of the checklist showing all documents submitted in case any document fails to upload successfully.

Grants.gov Helpdesk:

For assistance with Grants.gov, please call the Contact Center at +1 (800) 518-4726 or email support@grants.gov. The Contact Center is available 24 hours a day, seven days a week, except federal holidays. A full list of federal holidays can be found [here](#).

D4. Submission Dates and Times

Applications are due no later than 11:59 PM Eastern Daylight Time (DT), on Friday, 9 August 2024 via Grants.gov (<https://www.grants.gov/>), or MyGrants ([ILMS Service Portal - ILMS Support Desk \(servicenowservices.com\)](https://mygrants.service-now.com)), under the announcement title “FALCON” and funding opportunity number “DFOP0016632”.

Grants.gov and MyGrants automatically log the date and time an application submission is made, and the Department of State will use this information to determine whether an application has been submitted on time. Late applications are neither reviewed nor considered. Known system errors caused by Grants.gov or MyGrants (<https://mygrants.service-now.com>) that are outside of the applicant’s control will be reviewed on a case-by-case basis. Applicants should not expect a notification upon CDP receiving their application.

D5. Funding Limitations, Restrictions, and other Considerations

CDP will not consider applications that reflect any type of support for any member, affiliate, or representative of a designated terrorist organization. Please refer the link for Foreign Terrorist Organizations: <https://www.state.gov/foreign-terrorist-organizations/>

The Leahy Law prohibits Department foreign assistance funds from supporting foreign security force units if the Secretary of State has credible information that the unit has committed a gross violation of human rights. Per [22 USC §2378d\(a\) \(2017\)](#), “No assistance shall be furnished under this chapter [FOREIGN ASSISTANCE] or the Arms Export Control Act [22 USC 2751 et seq.] to any unit of the security forces of a foreign country if the Secretary of State has credible information that such unit has committed a gross violation of human rights.” Restrictions may apply to any proposed assistance to police or other law enforcement. Among these, pursuant to section 620M of the Foreign Assistance Act of 1961, as amended (FAA), no assistance provided through this funding opportunity may be furnished to any unit of the security forces of a foreign country when there is credible information that such unit has committed a gross violation of human rights. In accordance with the requirements of section 620M of the FAA, also known as the Leahy law, project beneficiaries or participants from a foreign government’s security forces may need to be vetted by the Department before the provision of any assistance. If a proposed grant or cooperative agreement will provide assistance to foreign security forces or personnel, compliance with the Leahy Law is required.

Organizations should be cognizant of these restrictions when reviewing and executing Project Activity Scopes as these restrictions will require appropriate due diligence of project beneficiaries and collaboration with CDP to ensure compliance with these restrictions. Project beneficiaries subject to due diligence vetting by the Department of State will include any individuals or entities that are beneficiaries of foreign assistance funding or support. Due diligence vetting will include a review of open-source materials.

D6. Other Submission Requirements

It is the responsibility of the applicant to ensure that it has an active registration in MyGrants or Grants.gov. Applicants are required to document that the application has been received by MyGrants or Grants.gov in its entirety. CDP bears no responsibility for disqualification that result from applicants not being registered before the due date, for system errors in either MyGrants or Grants.gov, or other errors in the application process.

Applicants are strongly encouraged to save a screen shot of the checklist showing all documents submitted in case any document fails to upload successfully.

Faxed, couriered, or emailed documents will not be accepted. Reasonable accommodations may, in appropriate circumstances, be provided to applicants with disabilities or for security reasons. **Applicants must follow all formatting instructions in the applicable NOFO and these instructions.**

CDP encourages organizations to **submit applications during normal business hours** (Monday – Friday, 9:00AM-5:00PM Eastern Time (EST or EDT as case may be)). If an applicant experiences technical difficulties and has contacted the appropriate helpdesk but is not receiving timely assistance (i.e., if you have not received a response within 48 hours of contacting the helpdesk), you may contact the CDP point of contact listed in in Section G for further assistance.

Section E: Application Review Information

E1. Application Review Criteria

The selected CDP review panel will evaluate each application individually against the following criteria, listed below in order of importance, and not against competing applications. Please use the below criteria as a reference, but **do not structure your application according to the sub-sections.**

Organizational and Technical Capacity (60 points)

- The applicant demonstrates highly developed administrative, logistical, and technical capacity and experience in administering successful and similar projects with a global participant base.
- The applicant proves existing, collaborative, and successful partnerships with U.S. and foreign partners on issues and engagements related to cybersecurity and digital policy.
- The applicant demonstrates capacity to deploy complex technical solutions in response to sophisticated cyber threat activity.
- The application demonstrates the organization's capacity for responsible fiscal management, technical equipment and software sourcing, federal contracting and logistics management.

Key Personnel (20 points)

- Key personnel have demonstrated experience and subject matter expertise as described in this announcement (see section D2.1.7 above).

Project Design, Monitoring and Evaluation (10 points)

- The applicant demonstrates the capacity to design projects that address the key objectives and activities for the target beneficiaries – as well as flexibility in deploying effective and durable solutions according to current understood best practices.
- The applicant demonstrates capacity to develop and execute logic models and monitoring and evaluation and report results.

Budget & Budget Narrative (10 points)

- The baseline budget justification is a detailed and realistic financial expression of the proposed project and does not include estimated costs that are not allocable, reasonable, or allowable.
- The applicant has included or described the organization's personnel policies for overtime and any other factors that may impact the budget given the rapid response nature of projects.

E2. Review and Selection Process

The Department of State is committed to ensuring a competitive and standardized process for awarding funding. Applications will be screened initially in a Technical Eligibility Review stage to determine whether applicants meet the eligibility requirements outlined in section C and have submitted all required documents outlined in section D. Applications that do not meet these requirements will not advance beyond

the Technical Eligibility Review stage and will be deemed ineligible for funding under this NOFO.

All applications that are deemed technically eligible will proceed to the Merit Review Panel consisting of U.S. government subject matter and/or country-specific experts and will be rated on a 100-point scale. CDP reserves the right to request the assistance of non-US government Subject Matter Experts (SMEs), if appropriate to the solicitation. Point values for individual elements of the application are presented in Section E.1. Panel Reviewers' ratings, and any resulting recommendations, are advisory. Panel Reviewers may provide conditions and recommendations on applications to enhance the proposed project, which must be addressed by the applicant before further consideration of the award.

Final selection authority resides with CDP's senior level official. Final award decisions will be influenced by whether the application meets the Department of State's programmatic goals and objectives, how it supports the Department's overarching foreign policy priorities.

E3. Responsibility/Qualification Information in SAM.gov (formerly, FAPIIS)

For any federal award under a notice of funding opportunity, if the federal awarding agency anticipates that the total federal share will be greater than the simplified acquisition threshold over the period of performance (see §200.01 Simplified Acquisition Threshold), this section must also inform applicants that:

- i. The Department of State, prior to making a federal award with a total amount of federal share greater than the simplified acquisition threshold, is required to review and consider any information about the applicant that is in the designated integrity and performance system accessible through SAM.gov (see 41 U.S.C. 2313);
- ii. The applicant, at its option, may review and comment on any information about itself that a federal awarding agency previously entered. Currently, federal agencies create integrity records in the integrity module of the Contractor Performance Assessment and Reporting System (CPARS) and these records are visible as responsibility/qualification records in SAM.gov;
- iii. The Department of State will consider any comments by the applicant, in addition to the other information in the designated integrity and performance system, in making a judgment about the applicant's integrity, business ethics, and record of performance under federal awards when completing the review of risk posed by applicants as described in §200.205 - Federal awarding agency review of risk posed by applicants.

Section F: Federal Award Administration Information

F1. Federal Award Notices

The Bureau of Cyberspace and Digital Policy (CDP) will provide a separate notification to applicants on the result of their applications. Successful applicants will receive a letter electronically via email including a request for the applicant respond to panel conditions and recommendations. This notification is **not** an authorization to begin activities and does not constitute formal approval or a funding commitment.

Final approval is contingent on the applicant successfully responding to the merit review panel's conditions and recommendations; being registered in required systems; and providing any additional completed documentation requested by CDP or the Grants Officer. Final approval is also contingent on Congressional Notification requirements being met and final review and approval by the Department's warranted Grants Officer.

The Notice of Award signed by the Department's warranted Grants Officers is the sole authorizing document. The recipient may only start incurring project expenses beginning on the start date shown on the grant award document signed by the Grants Officer. If awarded, the Notice of Award will be provided to the applicant's designated Authorizing Official via MyGrants to be electronically counter signed in the system.

Payments under this award will be made through the U.S. Department of Health and Human Services (HHS) Payment Management System (PMS). Unless otherwise stipulated, the Recipient may request payments on a reimbursement or advance basis. Instructions for requesting payments are available at: <https://pms.psc.gov/>.

Advance payments must be limited to the minimum amounts needed and be timed to be in accordance with the actual, immediate cash requirements of the Recipient in carrying out the purpose of this award. The timing and amount of advance payments must be as close as is administratively feasible to the actual disbursements by the Recipient for direct program or project costs and the proportionate share of any allowable indirect costs.

F2. Administrative, National Policy and Legal Requirements

Legal restrictions on foreign assistance are regularly updated. CDP requires all recipients of foreign assistance funding to comply with all applicable Department and federal laws and regulations, including but not limited to the following:

The Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards set forth in 2 CFR Chapter 200 (Sub-Chapters A through F) shall apply to all non-federal entities, except for assistance awards to Individuals and Foreign Public Entities. Sub-Chapters A through E shall apply to all foreign organizations, and Sub-Chapters A through D shall apply to all U.S. and foreign for-profit entities. The applicant/recipient of the award and any sub-recipient under the award must comply with all applicable terms and conditions, in addition to the assurance and certifications made part of the Notice of Award. The Department's Standard Terms and Conditions can be viewed at <https://www.state.gov/about-us-office-of-the-procurement-executive/>.

Before submitting an application, applicants should review all the terms and conditions and required certifications which will apply to this award, to ensure that they will be able to comply. These include:

- [2 CFR 25 – UNIVERSAL IDENTIFIER AND SYSTEM FOR AWARD MANAGEMENT](#)
- [2 CFR 170 – REPORTING SUBAWARD AND EXECUTIVE COMPENSATION INFORMATION](#)
- [2 CFR 175 – AWARD TERM FOR TRAFFICKING IN PERSONS](#)
- [2 CFR 182 – GOVERNMENTWIDE REQUIREMENTS FOR DRUG-FREE WORKPLACE \(FINANCIAL ASSISTANCE\)](#)
- [2 CFR 183 – NEVER CONTRACT WITH THE ENEMY](#)
- [2 CFR 600 – DEPARTMENT OF STATE REQUIREMENTS](#)
- [U.S. DEPARTMENT OF STATE STANDARD TERMS AND CONDITIONS](#)
-

In accordance with the Office of Management and Budget's guidance located at 2 CFR part 200, all applicable federal laws, and relevant Executive guidance, the Department of State will review and consider applications for funding, as applicable to specific programs, pursuant to this notice of funding opportunity in accordance with the following:

[Guidance for Grants and Agreements in Title 2 of the Code of Federal Regulations](#) (2 CFR), as updated in the Federal Register's 85 FR 49506 on August 13, 2020, particularly on:

- Selecting recipients most likely to be successful in delivering results based on the project objectives through an objective process of evaluating federal award applications (2 CFR part 200.205),
- Prohibiting the purchase of certain telecommunication and video surveillance services or equipment in alignment with section 889 of the National Defense Authorization Act of 2019 (Pub. L. No. 115—232) (2 CFR part 200.216),

- Promoting the freedom of speech and religious liberty in alignment with *Promoting Free Speech and Religious Liberty* (E.O. 13798) and *Improving Free Inquiry, Transparency, and Accountability at Colleges and Universities* (E.O. 13864) (§§ 200.300, 200.303, 200.339, and 200.341),
- Providing a preference, to the extent permitted by law, to maximize use of goods, products, and materials produced in the United States (2 CFR part 200.322), and
- Terminating agreements in whole or in part to the greatest extent authorized by law if an award no longer effectuates the program goals or agency priorities (2 CFR part 200.340).

In accordance with the Executive Order on Advancing Racial Equity and Underserved Communities, proposals should demonstrate how the project advances equity with respect to race, ethnicity, religion, income, geography, gender identity, sexual orientation, and disability. The proposal should also demonstrate how the project will further engagement in underserved communities and with individuals from underserved communities. Proposals should demonstrate how addressing racial equity and underserved communities will enhance the project's goals and objectives, as well as the experience of participants.

The support of underserved communities will be part of the review criteria for this opportunity. Therefore, proposals should clearly demonstrate how the project will support and advance equity and engage underserved communities in project administration, design, and implementation.

Due to the determination made under the Trafficking Victims Protection Act (TVPA) for FY 2021, assistance that benefits the governments of the following countries may be subject to a restriction under the TVPA. The Department of State determines on a case-by-case basis what constitutes assistance to a government; the general principles listed below apply.

Assistance to the government includes:

- All branches of government (executive, legislative, judicial) at all levels (national, regional, local).
- Public schools, universities, hospitals, and state-owned enterprises, as well as government employees.
- Cash, training, equipment, services, or other assistance provided directly to the government, assistance provided to an NGO or other implementer for the benefit of the government, and assistance to government employees.

F3. Reporting

Reporting is critical to effective project management and oversight. Reports are required as a means of evaluating the recipient's progress and utilization of resources. They are divided between a performance progress report and a financial status report. Applicants should be aware that CDP awards require that all reports (progress and financial) are uploaded to the grant file in MyGrants typically on a quarterly basis. The Federal Financial Report (FFR or SF-425) is the required form for the financial reports and must be submitted in PMS, as well as a copy from PMS then uploaded to the grant file in MyGrants. The progress reports uploaded to the grant file in MyGrants must include a narrative as described below and project indicators (or other mutually agreed upon format approved by the Grants Officer) for the F Framework and DCCP indicators. The F Framework indicators and DCCP indicators will be reviewed and negotiated during the final stages of issuing an award.

Financial Reports are also required on a quarterly basis (unless stipulated otherwise in the final Agreement), using form SF-425, the Federal Financial Report form. If payment is made through the Payment Management System, all financial reports must be submitted electronically through the Payment Management System. The Recipient is also required to upload to MyGrants a pdf version of all financial reports (Federal Financial Report) they have submitted in the Payment Management System. Form (SF-425) is located on the Post-Award Reporting forms page of [Grants.gov](https://www.grants.gov), linked here.

Final Reports

The final report will be due no later than 120 days after the end date of the award or termination of all project activities. The final report shall include the following elements: executive summary, successes, outcomes, best practices, how the project will be sustained, and a final Federal Financial Report (FFR). Additional guidance may be provided prior to the award end date.

Please note, delays in reporting may result in delays of payment approvals and failure to provide required reports may jeopardize the recipients' ability to receive future U.S. government funds. CDP reserves the right to request any additional programmatic and/or financial project information during the award period of performance.

Foreign Assistance Data Review (FADR)

As required by Congress, the Department of State must make progress in its efforts to improve tracking and reporting of foreign assistance data through the Foreign Assistance Data Review (FADR). The FADR requires tracking of foreign assistance activity data from budgeting, planning, and allocation through obligation and disbursement. Successful applicants will be required to report and draw down federal funding based on

the appropriate FADR Data Elements, indicated within their award documentation. In cases of more than one FADR Data Element, typically program or sector and/or regions or country, the successful applicant will be required to maintain separate accounting records.

Applicants should be aware of the post award reporting requirements reflected in [2 CFR 200 Appendix XII—Award Term and Condition for Recipient Integrity and Performance Matters](#).

Section G: Federal Awarding Agency Contacts

For technical submission questions related to this NOFO, please contact:

DCCP Foreign Assistance Team
 Digital Connectivity and Cybersecurity Partnership (DCCP)
 Unit of Strategic Planning and Communications (SPC)
 Bureau of Cybersecurity and Digital Policy (CDP)
DCCP-Info@state.gov

G1. Questions

Any prospective applicant who has questions concerning the contents of this NOFO must email the questions to the contacts listed above with the subject “**[Applicant Name] [FALCON].**” **by Monday 22 July 2024.** To maintain fairness and transparency in competition, CDP will not answer substantive NOFO questions except when posting questions and answers to the announcement page as described below.

All questions must be submitted via email to contact listed above by the deadline stated above. CDP will periodically create a document of submitted questions with answers and upload it and post them in grants.gov. Prospective applicants are advised to regularly review the announcement page in grants.gov for any updates. Note that once the NOFO deadline has passed, CDP staff may not discuss this competition with applicants until the review process has been completed.

Section H: Other Information

Applicants should be aware that CDP understands that some information contained in applications may be considered sensitive or proprietary and will make appropriate efforts to protect such information. However, applicants are advised that Department

of State cannot guarantee that such information will not be disclosed, including pursuant to the Freedom of Information Act (FOIA) or other similar statutes.

The information in this NOFO is binding and may not be modified by any CDP representative. Explanatory information provided by CDP that contradicts this language will not be binding. Issuance of this NOFO does not constitute an award commitment on the part of the U.S. government, nor does it commit the U.S. government to pay for costs incurred in the preparation and submission of proposals. Further, the U.S. government reserves the right to reject any or all proposals received.

In accordance with applicable federal awarding agency policy, applicants must disclose in writing any potential conflict of interest to the federal awarding agency or pass-through entity.

If an award is issued, the award recipient will receive the DCCP Messaging Manual and will be required to adhere to all relevant branding requirements identified therein, including style guidelines (consistent with U.S. Department of State style guidelines), branding and logo information, and other important references and resources for DCCP partners.

Additional background information on CDP and its efforts can be found on: [.](#)

CDP may require that award recipients enter into a Non-Disclosure Agreement for certain aspects of this project.

Attachments:

Required Attachments for Application Submission:

- Tab 1 - FALCON Detailed Budget – Baseline
- Tab 2 - FALCON Budget Narrative – Baseline
- Tab 3 - FALCON Strategic Scope of Work

Example Templates for Project Activities (Not part of submission)

- Tab 4 - FALCON Project Activity Scope
- Tab 5 - FALCON PAS Logic Model
- Tab 6 - FALCON Detailed Budget for PAS
- Tab 7 - FALCON PAS Performance Monitoring and Evaluation Plan

KEY TERMS AND DEFINITIONS

Activity: A specific action undertaken over a specific timeframe through which inputs are mobilized to produce specific outputs. An activity can be a sub-component of a program, project, or process.

Critical and Emerging Technologies (CET): Advanced Computing, Advanced Engineering Materials, Advanced Gas Turbine Engine Technologies, Advanced Manufacturing, Advanced and Networked Sensing and Signature Management, Advanced Nuclear Energy Technologies, Artificial Intelligence, Autonomous Systems and Robotics, Biotechnologies, Communication and Networking Technologies, Directed Energy, Financial Technologies, Human-Machine Interfaces, Hypersonics, Networked Sensors and Sensing, Quantum Information Technologies, Renewable Energy Generation and Storage, Semiconductors and Microelectronics, Space Technologies and Systems.

Goal: The highest-order outcome or end state to which a program, project, process or policy is intended to contribute.

Information and Communications Technology (ICT): Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g. microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).

Monitoring: An ongoing system of gathering information and tracking performance to assess progress against established goals and objectives. Monitoring provides an indication of progress against goals and indicators of performance, reveals whether desired results are occurring, and confirms whether implementation is on track.

Objective: A statement of the condition or state one expects to achieve toward accomplishing a program or project goal.

Outcome: A result or effect that may be *contributed to* by the program or project, or *attributable to* the program or project. Outcomes may be short-term or long-term, intended or unintended, positive or negative, direct or indirect.

Performance Indicators: Performance indicators measure a particular characteristic or dimension of a project's outputs or outcomes. Outputs are directly attributable to the project activities, while outcomes typically represent longer-term results to which a given program contributes but for which it is not solely responsible.

Program: A set of activities or projects that are typically implemented by several parties over an unspecified timeframe and may cut across sectors, themes, and/or geographic areas.

Project: A set of activities intended to achieve a defined product, service, or result within specified resources and implementation schedules. A set of projects makes up the portfolio of a program.